Amendments to the Claims:

1. (currently amended) A method of controlling access of network management requests directed to one or more network devices that participate in a virtual private network, the method comprising the computer-implemented steps of:

a network manager and a managed network device agreeing on a first mapping between securityNames and virtual private network identifiers;

storing, at the network manager, a translation table containing the first mapping of securityName values to corresponding virtual private network identifiers;

storing, at a managed network device, a view-based access control model table containing a second mapping of securityName values to corresponding MIB (Management Information Base) Views;

receiving at the managed network device a request[[,]] from ~~a first network device~~ the network manager, which is participating in a particular virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more ~~second~~ network devices participating in the particular virtual private network;

wherein the request contains a particular securityName value that is mapped to the particular virtual private network identifier in the first mapping;

~~determining an identifier of the virtual private network in the request to carry out the management protocol operation~~

at the managed network device, extracting the particular securityName value from the request and identifying, based on the particular securityName value that is

mapped in the second mapping, one or more corresponding particular MIB (Management Information Base) Views;

at the managed network device, identifying, based on the one or more corresponding particular MIB (Management Information Base) Views and from ~~among~~ a plurality of managed objects, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

in response to the request, providing to the ~~first network device~~ network manager access to only the subset of managed objects from the plurality of managed objects.

2. (canceled)

3. (currently amended) A method as recited in Claim 1, further comprising the steps of providing, at ~~one of~~ the managed network device[[s]], [[a]] the second mapping ~~of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects,~~ in the form of one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

4. (currently amended) A method as recited in Claim 1, further comprising the steps of providing, at ~~one of~~ the managed network device[[s]], one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the

corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

5. (currently amended) A method as recited in Claim 1, further comprising the steps of providing, at ~~one of~~ the managed network device[[s]], [[a]] the second mapping ~~of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects~~, and wherein the steps of identifying a subset of objects and providing ~~the request with~~ access comprise the steps of[[.]]:

determining whether the ~~identifier~~ securityName value from the request is in the second mapping;

when the securityName value from the request is in the second mapping:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the second mapping, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

6. (currently amended) A method as recited in Claim 1, further comprising the steps of providing, at ~~one of~~ the managed network device[[s]], [[a]] the second mapping ~~of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects,~~ in the form of one or more entries in a view-based access control model table that associate security name values to corresponding MIB (Management

Information Base) Views, and wherein the steps of identifying a subset of objects and providing ~~the request with~~ access comprise the steps of:

determining whether the ~~identifier~~ securityName value from the request is in the view-based access control model table;

when the ~~identifier~~ securityName value from the request is in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

7. (currently amended) A method as recited in Claim 1, further comprising the steps of providing, at ~~one of~~ the managed network device[[s]], one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of:

determining whether the ~~identifier~~ securityName value from the request is in the view-based access control model table;

when the identifier from the request is in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

8. (currently amended) A method as recited in Claim 1, further comprising the steps of:

providing, at ~~a network management station~~ the network manager that is communicatively coupled to the network devices, a mapping of a plurality of virtual private network identifiers to SNMPv3 securityNames;

providing, at the ~~network management station~~ network manager , an executable process that associates a virtual private network identifier with each SNMP request that is issued by the network management station to the network devices.

9. (currently amended) A method of controlling access of network management requests directed to one or more network devices that participate in a virtual private network, the method comprising the computer-implemented steps of:

receiving, from a network device participating in a virtual private network, a request to carry out a management protocol operation, wherein the request contains an identifier of the virtual private network in a security name value, wherein the

identifier contained in the request is based on a mapping of securityName values to corresponding virtual private network identifiers that was agreed upon by two or more network devices participating in the virtual private network;

extracting the security name value, which identifies the virtual private network, and determining a protocol operation that is embodied in the request;

using a view-based access control model, matching the security name value, which identifies the virtual private network, to a management information base view that corresponds to the requested operation;

processing the requested operation only if access is allowed to managed objects, in the management information base, that are associated with one or more network devices participating in the virtual private network, based on the management information base view matching the security name value that identifies the virtual private network.

10. (original) A method as recited in Claim 9, further comprising the steps of:

determining whether the request can be satisfied;

extracting the security name value from a context string in the request.

11. (original) A method as recited in Claim 10, wherein the matching step further comprises the steps of:

determining whether the security name is in a view-based access control model table;

rejecting and returning the request when the security name is not found in the view-based access control model table.

12. (original) A method as recited in Claim 10, further comprising the steps of:

determining whether the security name is in a view-based access control model table;

when the security name is found in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the view-based access control model table, determining whether the protocol operation is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

13. (previously presented) The method as recited in Claim 10, further comprising the steps of:

determining whether the security name is in a view-based access control model table;

when the security name is found in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the view-based access control model table, determining whether the protocol operation is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable;

determining whether a virtual private network identifier is referenced in the request, processing the request using managed information objects in a default view when no virtual private network identifier is referenced in the request, and processing the request using management information objects in a view corresponding to the virtual private network identifier only when a virtual private network identifier is referenced in the request.

14. (currently amended) A computer-readable medium carrying one or more sequences of instructions for controlling access of network management requests directed to one or more network devices that participate in a virtual private network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

a network manager and a managed network device agreeing on a first mapping between securityNames and virtual private network identifiers;

storing, at the network manager, a translation table containing the first mapping of securityName values to corresponding virtual private network identifiers;

storing, at a managed network device, a view-based access control model table containing a second mapping of securityName values to corresponding MIB (Management Information Base) Views;

receiving at the managed network device a request[[,]] from ~~a first network device~~ the network manager, which is participating in a particular virtual private network, to carry out a management protocol operation that involves one or

more managed objects associated with one or more ~~second~~ network devices participating in the particular virtual private network;

wherein the request contains a particular securityName value that is mapped to the particular virtual private network identifier in the first mapping;

~~determining an identifier of the virtual private network in the request to carry out the management protocol operation~~

at the managed network device, extracting the particular securityName value from the request and identifying, based on the particular securityName value that is mapped in the second mapping, one or more corresponding particular MIB (Management Information Base) Views;

at the managed network device, identifying, based on the one or more corresponding particular MIB (Management Information Base) Views and from ~~among~~ a plurality of managed objects, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

in response to the request, providing to the ~~first network device~~ network manager access to only the subset of managed objects from the plurality of managed objects.

15. (canceled)

16. (currently amended) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at ~~one of~~ the managed

network device[[s]], [[a]] the second mapping ~~of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects,~~ in the form of one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

17. (currently amended) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at ~~one of~~ the managed network device[[s]], one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

18. (currently amended) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at ~~one of~~ the managed network device[[s]], [[a]] the second mapping ~~of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects~~, and wherein the steps of identifying a subset of objects and providing ~~the request with~~ access comprise the steps of[[.]]:

determining whether the ~~identifier~~ securityName value from the request is in the second mapping;

when the securityName value from the request is in the second mapping:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the second mapping, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

19. (currently amended) An apparatus for controlling access of network management requests directed to one or more network devices that participate in a virtual private network, comprising:

means for a second managed network device agreeing with a first network device on a first mapping between securityNames and virtual private network identifiers;

means for storing, at the second managed network device, a view-based access control model table containing a second mapping of securityName values to corresponding MIB (Management Information Base) Views;

means for receiving at the second managed network device a request[[,]] from ~~a first network device~~ the first network device, which is participating in a particular virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more ~~second~~ network devices participating in the particular virtual private network;

wherein the request contains a particular securityName value mapped, in the first mapping, to the particular virtual private network identifier, and wherein the first mapping is stored at the first network device;

~~means for determining an identifier of the virtual private network in the request to carry out the management protocol operation~~

at the second managed network device, means for extracting the particular securityName value from the request and identifying, based on the particular securityName value that is mapped in the second mapping, one or more corresponding particular MIB (Management Information Base) Views;

at the second managed network device, means for identifying, based on the one or more corresponding particular MIB (Management Information Base) Views and from ~~among~~ a plurality of managed objects, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

means for providing to the first network device access to only the subset of managed objects from the plurality of managed objects.

20. (currently amended) An apparatus controlling access of network management requests directed to one or more network devices that participate in a virtual private network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

a second managed network device agreeing with a first network device on a first mapping between securityNames and virtual private network identifiers;

storing, at the second managed network device, a view-based access control model table containing a second mapping of securityName values to corresponding MIB (Management Information Base) Views;

receiving at the second managed network device a request[[,]] from ~~a first network device~~ the first network device, which is participating in a particular virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more ~~second~~ network devices participating in the particular virtual private network;

wherein the request contains a particular securityName value mapped, in the first mapping, to the particular virtual private network identifier, and wherein the first mapping is stored at the first network device;

~~determining an identifier of the virtual private network in the request to carry out the management protocol operation~~

at the second managed network device, extracting the particular securityName value from the request and identifying, based on the particular securityName value that is mapped in the second mapping, one or more corresponding particular MIB (Management Information Base) Views;

at the second managed network device, identifying, based on the one or more corresponding particular MIB (Management Information Base) Views and from ~~among~~ a plurality of managed objects, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

providing to the first network device access to only the subset of managed objects from the plurality of managed objects.

21. (previously presented) A method of controlling access of network management requests directed to one or more network devices that participate in one or more virtual private networks, the method comprising the computer-implemented steps of:

receiving a request to carry out a SNMP (Simple Network Management Protocol) operation directed to one or more managed objects from a MIB (Management Information Base) associated with one or more network devices that participate in multiple virtual private networks;

determining, from the request, an identifier of a particular virtual private network of the multiple virtual private networks;

identifying, among a plurality of managed objects from a MIB associated with a network device from the one or more network devices that participate in the multiple virtual private networks, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

in response to the request, providing access to only the subset of managed objects.

22. (new) The apparatus of Claim 19, further comprising means for providing, at the managed network device, the second mapping in the form of one or more entries in a

view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

23. (new) The apparatus of Claim 19, further comprising means for providing, at the managed network device, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

24. (new) The apparatus of Claim 19, further comprising means for providing, at the managed network device, the second mapping, and wherein the means for identifying a subset of objects and providing access comprise:

means for determining whether the securityName value from the request is in the second mapping;

means for identifying a management information base variable referenced in the request when the securityName value from the request is in the second mapping;

based on one or more views referenced in the second mapping, means for determining whether a protocol operation of the request is allowed for the variable when the securityName value from the request is in the second mapping;

means for dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable when the securityName value from the request is in the second mapping.

25. (new) The apparatus of Claim 19, further comprising means for providing, at the managed network device, the second mapping in the form of one or more entries in a view-based access control model table that associate security name values to corresponding MIB (Management Information Base) Views, and wherein the means for identifying a subset of objects and providing access comprise:

means for determining whether the securityName value from the request is in the view-based access control model table;

means for identifying a management information base variable referenced in the request when the securityName value from the request is in the view-based access control model table;

based on one or more MIB Views referenced in the view-based access control model table, means for determining whether a protocol operation of the request is allowed for the variable when the securityName value from the request is in the view-based access control model table;

means for dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable when the securityName value from the request is in the view-based access control model table.

26. (new) The apparatus of Claim 19, further comprising means for providing, at the managed network device, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is

associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks, and wherein the means for identifying a subset of objects and providing the request with access comprise:

means for determining whether the securityName value from the request is in the view-based access control model table;

means for identifying a management information base variable referenced in the request when the identifier from the request is in the view-based access control model table;

based on one or more MIB Views referenced in the view-based access control model table, means for determining whether a protocol operation of the request is allowed for the variable when the identifier from the request is in the view-based access control model table;

means for dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable when the identifier from the request is in the view-based access control model table.

27. (new) The apparatus of Claim 19, further comprising:

means for providing, at the network manager that is communicatively coupled to the network devices, a mapping of a plurality of virtual private network identifiers to SNMPv3 securityNames;

means for providing, at the network manager, an executable process that associates a virtual private network identifier with each SNMP request that is issued by the network management station to the network devices.

28. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of providing, at the managed network device, the second mapping in the form of one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

29. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of providing, at the managed network device, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

30. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of providing, at the managed network device, the second mapping, and wherein the steps identifying a subset of objects and providing access comprise:

determining whether the securityName value from the request is in the second mapping;

when the securityName value from the request is in the second mapping:

identifying a management information base variable referenced in the request ;

based on one or more views referenced in the second mapping, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

31. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of providing, at the managed network device, the second mapping in the form of one or more entries in a view-based access control model table that associate security name values to corresponding MIB (Management Information Base) Views, and wherein the steps of identifying a subset of objects and providing access comprise:

determining whether the securityName value from the request is in the view-based access control model table;

when the securityName value from the request is in the second mapping:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

32. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of providing, at the managed network device, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks, and wherein the steps of identifying a subset of objects and providing the request with access comprise:

determining whether the securityName value from the request is in the view-based access control model table;

when the identifier from the request is in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

33. (new) The apparatus of Claim 20, wherein the one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

providing, at the network manager that is communicatively coupled to the network devices, a mapping of a plurality of virtual private network identifiers to SNMPv3 securityNames;

providing, at the network manager, an executable process that associates a virtual private network identifier with each SNMP request that is issued by the network management station to the network devices.